AFRL-RI-RS-TR-2017-029

IMPROVING CYBERSECURITY INCIDENT RESPONSE TEAM (CSIRT) SKILLS, DYNAMICS AND EFFECTIVENESS

DARTMOUTH COLLEGE

MARCH 2017

FINAL TECHNICAL REPORT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

STINFO COPY

AIR FORCE RESEARCH LABORATORY
INFORMATION DIRECTORATE

■ **AIR FORCE MATERIEL COMMAND** ■ **UNITED STATES AIR FORCE** ■ **ROME, NY 13441**

NOTICE AND SIGNATURE PAGE

Using Government drawings, specifications, or other data included in this document for any purpose other than Government procurement does not in any way obligate the U.S. Government. The fact that the Government formulated or supplied the drawings, specifications, or other data does not license the holder or any other person or corporation; or convey any rights or permission to manufacture, use, or sell any patented invention that may relate to them.

This report is the result of contracted fundamental research deemed exempt from public affairs security and policy review in accordance with SAF/AQR memorandum dated 10 Dec 08 and AFRL/CA policy clarification memorandum dated 16 Jan 09. This report is available to the general public, including foreign nationals. Copies may be obtained from the Defense Technical Information Center (DTIC) (http://www.dtic.mil).

AFRL-RI-RS-TR-2017-029 HAS BEEN REVIEWED AND IS APPROVED FOR PUBLICATION IN ACCORDANCE WITH ASSIGNED DISTRIBUTION STATEMENT.

FOR THE CHIEF ENGINEER:

/ S /
ROBERT KAMINSKI
Work Unit Manager

/ S /
WARREN H. DEBANY, JR.
Technical Advisor, Information
Exploitation and Operations Division
Information Directorate

This report is published in the interest of scientific and technical information exchange, and its publication does not constitute the Government's approval or disapproval of its ideas or findings.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
FEBRUARY 2017	FINAL TECHNICAL REPORT	SEP 2012 – JUN 2016

4. TITLE AND SUBTITLE

IMPROVING CYBERSECURITY INCIDENT RESPONSE TEAM (CSIRT) SKILLS, DYNAMICS AND EFFECTIVENESS

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
FA8750-12-2-0258

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Shari Lawrence Pfleeger

5d. PROJECT NUMBER
DHS2

5e. TASK NUMBER
DA

5f. WORK UNIT NUMBER
RT

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Trustees of Dartmouth College
Office of Sponsored Projects
Hanover, NH 03755-1404

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Air Force Research Laboratory/RIG
525 Brooks Road
Rome NY 13441-4505

10. SPONSOR/MONITOR'S ACRONYM(S)
AFRL/RI

11. SPONSOR/MONITOR'S REPORT NUMBER
AFRL-RI-RS-TR-2017-029

12. DISTRIBUTION AVAILABILITY STATEMENT
Approved for Public Release; Distribution Unlimited. This report is the result of contracted fundamental research deemed exempt from public affairs security and policy review in accordance with SAF/AQR memorandum dated 10 Dec 08 and AFRL/CA policy clarification memorandum dated 16 Jan 09.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

By analyzing documentation, observing actual CSIRT activity, convening focus groups, and using pre- and post-incident interviews, a team from Dartmouth College, George Mason University and Hewlett-Packard recommended ways to improve the skills, dynamics and effectiveness of CSIRTs. The results include descriptions of needed knowledge, skills and abilities for key CSIRT roles, viewed from individual, team and multi-team system perspectives, as well as simulation-derived recommendations for optimal CSIRT performance.

15. SUBJECT TERMS

Cyber Incident Response, Response Teams, Cognitive Task Analysis

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			**ROBERT KAMINSKI**
U	U	U	UU	21	19b. TELEPHONE NUMBER (*Include area code*) **N/A**

TABLE OF CONTENTS

1.0 Summary

The effectiveness of CSIRTs rests on both technological and social capacities. Both are necessary; neither is sufficient. Yet despite the joint importance of these capacities, most handbooks and training programs designed to increase CSIRT effectiveness focus mainly on technology. When "team" aspects of computer security incident response are addressed in existing work, the emphasis is typically on individual functions and incident response process flow. This research project responds to the growing sense among CSIRT professionals that human tech savvy is increasingly not enough; and it is certainly not scalable in lock-step with the outgrowth of cyber threats.

The resulting volume from this research project is written precisely to address this challenge, and, above all, to answer the question: *How does a CSIRT manager assemble and cultivate a team capable of delivering effective cybersecurity incident response?*

What constitutes good performance among cybersecurity incident responders is not well understood. The research summarized in this body of work identified several social processes and dynamics that contribute to incident response effectiveness. *The resulting Handbook, at the most practical level, seeks to provide a baseline for achieving effective CSIRT performance.* It provides the methods and strategies necessary to build, staff, train, and foster a team that leverages both the latest technologies and the social dynamics required to make the best use of them.

A sophisticated, high-performing CSIRT is not just a single team, but rather, a closely connected network of teams. Such component teams are often identified by function within the overall CSIRT, such as forensics or threat intelligence. This network of teams is known as a multiteam system, or MTS. This concept was emphasized throughout this project. When reading the chapters in the Handbook, it is important to keep in mind that building a productive CSIRT requires not just collaboration between individual team members, but collaboration among the component teams as well. The success of a CSIRT can hinge on these MTS interactions: a CSIRT can have strong collaborative bonds within the team, or be well-led overall, but still fail due to mistrust or lack of communication among individual CSIRT component teams.

The dynamic nature of an MTS, in particular, means that CSIRT managers must develop a firm understanding of the social dynamics that drive people in a complex organization. This is especially important when considering that MTSs are the future of cyber incident response and must become as operationally agile as the evolving threat. Several recommendations to address complex MTS challenges appeared based on this research project including mapping the team relationships within the CSIRT, assessing the social maturity of the overall CSIRT team and the MTS relationships, greater use of situational interviewing and emphasizing common or shared goals among the CSIRT MTS. Details of the recommendations and this project's full research findings can be found in the complete Handbook at http://calctraining2015.weebly.com/the-handbook.html

2.0 Introduction

Cybersecurity in the twenty-first century reflects the most technologically sophisticated threat environment the world has ever seen. Cyber incidents are asymmetric and evolving – threatening institutions, individuals, organizations, and governments. The familiar refrains "attribution is difficult" and "the threat is amorphous" have become the stuff of industry lore. In this environment, organizations frequently seek to stay ahead of the threat by maintaining a distinct technological advantage. This advantage has long been accepted as a given considering the history and evolution of the cyber domain. The Western world not only invented the Internet and the systems that form its architecture, but institutions of higher education have responded by producing human talent that is adept at using the latest technologies. Our tools are second-to-none, and our capacity to train people in the use of these tools has never been greater.

Yet, the technological edge enjoyed by organizations in developed nations is diminishing as the world further integrates its knowledge. Furthermore, while technology enjoys pride of place in any conversation on cybersecurity, technology is only part of the solution to real-time cybersecurity. Technology relies upon the people behind it, and because cybersecurity incident response increasingly requires collective action, this creates an entirely new paradigm for cybersecurity. The latest technologies remain bound to human social dynamics and approaches to collective problem-solving that pre-date our species' mastery of fire.

In short, social dynamics are more important than ever, particularly in the practice of cybersecurity incident response, which requires a well-managed, skilled and efficient Cybersecurity Incident Response Team (CSIRT). For CSIRT managers, finding the right mixture of talent and creating the right social dynamics is both imperative and increasingly challenging. Cybersecurity incident responders often need to work within volatile, uncertain, complex, and ambiguous environments. So much of the counterintuitive skillset that makes a good analyst – creative problem-solving, outside-the-box thinking, and subject expertise – reflects a mosaic of skills that make traditional notions of collaboration challenging.

For managers, building CSIRTs that can maintain tight time constraints and achieve data accuracy, all while working in an evolving threat landscape, will require a renewed focus on team building and collective problem-solving. Such a complex environment, and its many challenges, launched this research.

3.0 Methods, Assumptions, and Procedures

This project and the resulting Handbook was jointly funded by the U.S. Department of Homeland Security (DHS), the National Cyber Security Centre (NCSC) of the Netherlands, and the Swedish Civil CONTINGENCIES Agency (MSB). This effort joined scientists from three institutions, George Mason University, Dartmouth College, and Hewlett-Packard, to create a large multidisciplinary research team.

One purpose of our research effort was to examine CSIRT MTSs that are typically used to resolve cybersecurity incidents. Another purpose was to define the planning processes, behaviors, and outcomes that reflect successful CSIRT performance at the individual, team, and MTS level. Several projects comprised our research effort (details of each can be found in the chapters and/or appendices of the Handbook at http://calctraining2015.weebly.com/the-handbook.html, including:

- **Construction and Validation of an Incident Response Performance Taxonomy**. Our research team developed a taxonomy of cybersecurity incident response performance, which indicates three dimensions of performance: *level* (individual, team, MTS), *timing* (proactive versus reactive processes), and *performance phase* (planning versus execution activities). We used this taxonomy to derive Knowledge, Skills, Abilities, and Other attributes (KSAOs) necessary for effective cybersecurity performance.
- **Review of Existing CSIRT Research**. Our research team undertook a comprehensive review of existing academic and applied research on CSIRT effectiveness, which contributed to the construction of the taxonomy of cybersecurity incident response performance.
- **Review of Existing CSIRT Job Analyses**. In developing a job analysis, our team conducted a study of the cognitive, social, personality, and motivational requirements involved in cybersecurity incident response and then validated our conclusions against several existing analyses in the field.
- **Review of Job Ads for CSIRT Positions**. Our team reviewed over 100 job advertisements for cybersecurity personnel hires and identified (a) the KSAOs typically sought by cybersecurity managers and (b) the gaps between such KSAOs and those attributes identified as important in our research.
- **Focus Group Interviews.** Our research involved one of the most comprehensive sets of interviews of incident responders in a single study. We conducted 52 focus group interviews with a total of approximately 150 participants. We also interviewed 28 representatives of CSIRT MTSs. The interviews included CSIRTs from 17 organizations across the United States, the United Kingdom, Germany, Sweden, and the Netherlands. The types of CSIRTs represented in our sample included government CSIRTs, military CSIRTs, managed security provider CSIRTs corporate CSIRTs, and academic institution CSIRTs.
- **Survey of Non-Technical KSAOs.** Previous known studies of CSIRTs did not examine cognitive, social, and character attributes that influence CSIRT performance. As part of this effort, we developed a comprehensive list of such attributes from our taxonomy, our focus group interviews, and from a survey of 88 CSIRT professionals.
- **Cognitive Task Analysis**. Most job analyses focus on the behaviors required for job performance. However, because our taxonomy indicated the centrality of knowledge work in incident response, we also conducted a cognitive task analysis (CTA) designed to identify the particular cognitive skills that contribute to effective CSIRT performance.
- **MTS Analysis**. As discussed in the introduction, a key aspect of our research was to examine CSIRTs as MTSs. Different processes and team dynamics are relevant for MTSs that are not equally relevant for traditional teams. An MTS does not simply refer to a collection of teams working in a CSIRT, but highlights the fact that in CSIRT MTSs, component teams collaborate closely to solve complex problems. This concept in organizational science has been applied to many organizational settings, including military, health, transportation, business, and disaster recovery. We have applied it to the domain of cybersecurity incident response. As part of this effort, we analyzed the elements of 28 incident response MTSs.

4.0 Results and Discussion

This section presents ten key areas summarizing our major findings and recommendations. More detailed discussion of these findings as well as assessment exercises and improvement strategies to assist CSIRT managers in evaluating and improving their teams are included in the chapters and appendices of the Handbook, which can be accessed at http://calctraining2015.weebly.com/thehandbook.html

Social Maturity of Teams. CSIRTs are composed primarily of multiteam systems (MTSs), which are a closely connected network of teams working together to accomplish a common goal. MTSs represent a dynamic and necessary organizational structure for cyber incident response, but MTSs also present complex challenges for CSIRT managers. Our research found that in some instances, when cyber analysts believe they are part of a strong team, they may not as readily trust other teams in the MTS, weakening the MTS as a whole. This frequently requires CSIRT managers to improve communications between teams and identify areas for improvement across the MTS. Conversely, our research also suggests that a strong MTS can often obscure the weaknesses of individual teams. It can actually become more challenging for CSIRT managers to fix the weaknesses of individual teams because the urgency is not as apparent. CSIRT managers must maintain insight into the performance of both individual teams and the broader MTS. Frequently, MTS performance can suffer when teams lack the social maturity to collaborate in the resolution of incidents. Social Maturity is the degree to which a team has the capacity for its members to collaborate in completing the team's mission. Our research found that collaboration can be improved and team performance can be optimized, when CSIRT managers:

- *Map Their MTS.* This starts with recognizing that their CSIRT is a connected set of teams. It also requires maintaining awareness of both the differing level of interaction between teams, and that these interactions change during higher impact, or more severe, events.
- *Assess the Social Maturity of Each CSIRT Component Team and the Overall CSIRT MTS.* Key team attributes a manager should assess include: collaboration triggering, communication skills and protocols, information sharing, collaborative problem-solving, shared knowledge of unique expertise, trust, adaptation, collective learning, and conflict management.
- *Use Situational Interviews to Make Staffing Decisions and Assess Group Work Preferences.* Managers should ask job candidates a standard set of questions focused on past behaviors and experiences that will illuminate a candidate's ability to work effectively in a group environment.
- *Focus on Emphasizing Distal Goal Commitment.* CSIRT managers must be advocates for focusing on the goals of the entire CSIRT MTS. Component teams frequently focus on their own goals. CSIRT managers must counteract this tendency by emphasizing common or shared goals.
- *Encourage Regular Cross-Team Connections.* Managers must create opportunities and settings for more communication between different teams.

CSIRT Performance Evaluation. An effective performance measurement and evaluation program can greatly benefit CSIRTs by providing information on individual, team, and MTS behavior that reflect successful job performance. Establishing clear performance metrics can measure the efficiency, effectiveness, value, or impact of an employee's action. Our research found that – especially in light of the diverse composition of a CSIRT and the social maturity required of its teams – performance metrics and evaluation are essential toward constantly improving performance outcomes. A Performance

Measurement Program is never static, but our research found that five strategies are instrumental to a successful CSIRT Performance Measurement Program:

- *Balancing Measuring Quantity and Quality.* Quantity falls under objectively-derived metrics, and quality often requires managerial and client ratings. CSIRT managers can use their discretion to determine the balance needed when measuring the quality and quantity of job behaviors; however, the only caution is not to allow metrics along to guide performance evaluation. Given the imperative of collaboration and communication within an MTS, client ratings can be uniquely useful for CSIRT members.
- *Measure Maximum Performance in Addition to Typical Performance.* In addition to typical performance, which is what managers usually measure, maximum performance can and should be measured through performance on periodically scheduled exercises and simulations. This will allow managers to understand the extent of their team's capabilities.
- *Measure both Proactive and Reactive Performance.* Every CSIRT manager to whom we spoke confirmed that an appreciable portion of CSIRT tasks involved proactive behavior. Yet, most CSIRTs often skew measurement to reactive performance. Managers should therefore supplement reactive performance metrics with proactive performance metrics.
- *Determine the Appropriate Level of Measurement.* The purpose of measuring performance should guide a CSIRT manager's approach. If the manager wants to determine the strongest and weakest members of a CSIRT, the individual level is most appropriate. If a manager wants to identify strengths and weaknesses of teamwork, the team or MTS level is most appropriate.
- *Create a Balanced Scorecard for Performance Measurement.* Our research found that one tool that can help a CSIRT manager maintain a comprehensive approach to performance measurement is known as the balanced scorecard. The balanced scorecard is not only a dashboard of metrics to measurement performance, but it can also suggest the relationship between categories of performance.

Decision-making in CSIRTs. Our research found that for every incident response trigger, there is an initial decision regarding whether to tend to the event. If the decision is made to act rather than categorize the event as a false positive, there are numerous subsequent decisions that must be made, including how to prioritize the event. Also, analysts must decide when it is appropriate to call on others to collaborate in order to mitigate the incident (referred to as collaboration triggering). Analysts must know when initiation of collaboration is necessary and when it is unnecessary, such as when the incident is routine. The effectiveness of these decisions depends upon a cybersecurity analyst's abilities. Our research found the following strategies for improved decision-making.

- *Selecting for Decision-Making Skills.* CSIRT managers should select applicants for their decision-making skills, particularly those involving problem sensitivity, critical thinking, and information ordering. The chapter on decision-making in the Handbook includes questions to facilitate this selection.
- *Training Decision-Making Skills*. We found that structured troubleshooting, critical thinking training, and expert modeling can alleviate the weaknesses in a novice's decision-making. Expert modeling in particular – which pairs a novice with an expert to resolve an incident unfamiliar to the novice – can improve the novice's abilities and team performance.

- *Cognitive Prompts for Expert Analysts*. Cognitive prompts can reduce overconfidence and information bias. One such strategy is the "Five-Why Analysis," developed by Toyota and used widely by a range of companies including Amazon.com. It involves asking "Why?" a particular incident happened and applying the same question five times to each answer. In cybersecurity, five-why analysis is believed to be more effective for use by teams of cybersecurity analysts rather than individual team members. Another strategy, "the pre-mortem," asks analysts to imagine they have already attempted to resolve the incident but have failed. They are then asked to identify the reasons why the incident response effort may have failed.
- *Using Mnemonics to Capture Necessary Information*. Mnemonics facilitate the use of protocols that remind the decision-maker to consider different aspects of a new situation. A widely used mnemonic in healthcare is SBAR, which stands for Situation, Background, Assessment, and Recommendations. SBAR has been shown to improve the communication of patient information among healthcare staff in a number of studies.
- *Using Adaptive Case Management*. In contrast to process models, an adaptive case management system focuses on the individual case – that is, the incident. Rather than prescribing general processes that the analyst is expected to follow, an AACM system provides context surrounding the incident by summarizing the ways in which similar incidents were handled in the past and the extent to which those ways proved successful.

Communication Effectiveness. Our study found that cybersecurity analysts rated communication skills at the top of social skills needed for CSIRT effectiveness. Three common challenges to communication effectiveness in CSIRTs include time demands, team member physical distance, and the need to communicate across cultural boundaries. To promote communication effectiveness, CSIRT managers need to ensure messages are clear in meaning, relevant in content, as well as appropriately timed, sent to the correct person, and acknowledged by recipients. Effective communication serves as a foundation for information sharing across individuals, teams, and MTSs.

- CSIRT managers can improve communication in their teams and MTSs by using aids such as communication charters, handoff checklists, virtual displays, and wikis.
- CSIRT managers can facilitate use of communication aids through scenario-based practice exercises and team simulations.
- CSIRT managers can enhance communication between teams by designating a specific person for each component team responsible for such communication.
- Careful design of physical workspaces can facilitate more frequent communications and sharing of information with appropriate stakeholders.

Information Sharing. Information sharing, in the realm of cybersecurity reflects the exchange of incident knowledge and threat data across and within organizations. The *type* of information shared, *with whom* information is to be shared, as well as both the *speed* and *accuracy* by which information is communicated before, during, and after an incident help determine the quality of responses to both familiar and novel incidents. Focusing on parameters of information sharing enables managers to identify effective strategies for improving CSIRT processes and performance. As examples, our research found that mandatory information sharing regulations should clearly define *how much of what type of communication should be communicated by when and to whom.* Managers should not discourage the discretionary sharing of information, as such activities promote collaboration. Managers also need to establish specific communication protocols based on various levels of information sharing (e.g., two individuals, with team, intra- or inter-organizational); different strategies for improving information

sharing might work at one level but not at another level. When individual-to-individual information sharing occurs, confirmation and response is fairly straightforward. However, when an individual sends information to an entire team, MTS, organization, or outside organization, responsibility for confirmation and response might not be clear.

To facilitate information sharing, CSIRT managers need to establish communication protocols and charters that do the following:

- Identify the recipients who would most benefit or require the information being shared;
- Consider carefully what information and how much recipients need in order to accomplish their work;
- Set norms for review of information posted for accuracy and completeness;
- Specify communication methods that allow confirmation of receipt to ensure information was received;
- Provide sender contact information, along with an invitation to request additional information, if necessary;
- Set communication norms within teams that support sharing of discretionary information:
    - When in the incident response cycle information should be sent; o What information is necessary for recipients;
    - When particular types of information are needed by others; o What types of information are necessary to share during high impact events; o How much information is sufficient to create situational awareness?
- In the case of mandatory information sharing, have regulations that clearly define *how much of what type of information should be communicated by when and to whom:*
    - Managers should revise the regulations and protocols that determine the mandatory sharing of information if they receive reports that information being sent under specific rules is consistently incomplete, irrelevant, inaccurate, not timely, or sent too infrequently (or too frequently).
- In the case of information sharing between individuals, teams, MTSs, organizations, or external stakeholders:
    - Define what kinds of information need to be shared with each. o Establish guidelines about which members within a team should respond to which kind of information sent to the entire team (based on knowledge).
    - Establish boundary spanners, or individuals tasked with responding when information sharing occurs between teams in an MTS or between organizations.

Managers should use guided simulations and scenarios to practice the use of communication charters and protocols to develop a shared understanding within the CSIRT of how information sharing at multiple levels should occur.

Collaborative Problem-Solving. The nature of CSIRT work is knowledge work that typically involves multiple team members working together to solve complex problems. CSIRTs must be able to engage in the process of situational awareness, collective information processing, and forecasting, in order to be effective in solving novel problems. Our research found that managers can improve these processes using strategies such as pre-briefing, debriefing, simulations, and giving focused feedback. Our interviews with CSIRT analysts and managers consistently indicated a higher percentage of endorsement of collaborative problem-solving steps between teams versus within teams, which supports our broader research finding that CSIRTs are often MTSs, conducting problem-solving as closely-knit interdependent teams. Further, our survey of critical knowledge, skills, abilities and other attributes that contribute to effective incident response indicated two problem-solving skills were in the top 10 highest rated

attributes. Skill in reviewing information to develop and implement solutions to complex problems ranked fifth highest in importance, and skill in working with other members to solve problems and come to solutions that will help the team ranked tenth highest. The following strategies were identified to enhance collaborative problem-solving:

- *Engage in pre-mission planning (or "pre-briefing").* CSIRT members cannot resolve an incident if they cannot define the problem parameters. Managers should lead a prebriefing to create a shared understanding of the problem, a shared understanding of the goal or desired outcome, and a shared understanding of the solution strategy. Contingency planning – a variation of pre-briefing – can help teams and CSIRTs anticipate unexpected events by planning how they will be handled in advance.
- *Use counterfactual thinking to get team members to share their unique information.* Team members often do not realize that they have information no one else knows. Managers should ask their team members to consider what might have happened in a past situation or a give scenario that is different from what actually happened. This often elicits unique information that individuals would not otherwise share in a group dynamic.
- *Provide team feedback during structured debriefing.* After incidents occur, and even after simulations, feedback during debrief is extremely important. It has been shown to improve team performance 19% more than teams who did not receive feedback. Managers or facilitators who are responsible for providing feedback should focus on teamwork successes as well as failures.
- *Develop adaptive thinking by providing exploratory or active learning experiences with wide problem variety.* Managers can use forms of exploratory or active learning to develop adaptive thinking skills. Managers should encourage team members to change how they are thinking about a particular problem by using such frame-changing prompts as "How is this problem different from other problems you faced?" or "What other possible solutions might apply to this problem?"
- *For MTSs, train leaders to pre-plan strategies for how multiple teams will work together.* MTS problem-solving can also be improved using the pre-planning strategies discussed earlier. Team leaders in an MTS can work together to engage in pre-planning that maps out (a) how multiple teams will work together, and (b) how each of those teams will coordinate their actions with other specific teams.
- *When staffing, build your CSIRT with team members who have a team orientation and teamwork skills.* A well thought out staffing plan can increase the effectiveness of team collaboration and collective problem-solving. Having high levels of team skills such as cooperativeness, team orientation, and organization skills will enable the team to build the levels of trust and SKUE (shared knowledge of unique expertise) that will foster effective collaborative problem-solving.

Shared Knowledge of Unique Expertise. By necessity, CSIRTs need a diverse collection of members with different perspectives and expertise to respond to ever-evolving incidents. This makes shared knowledge of unique expertise (SKUE) vital for CSIRT operations. Called "transactive memory" by some, SKUE reflects the idea that all CSIRT team members and MTS components must possess the same knowledge of "who knows what" to work efficiently. SKUE decreases the time it takes for CSIRT members to identify who has the knowledge that is needed, resulting in more effective collaboration. In 80% of the focus groups we conducted, knowing who had what expertise on the team was among the most important team attribute for CSIRT effectiveness. Knowing what other members across component teams know quickens the incident response process, including the identification and mitigation of threats. We found that two strategies in particular could help optimize SKUE in CSIRTs.

- *Establish knowledge tools (e.g., information board, knowledge map) that display members' expertise, knowledge, skills and experiences.*
- *Train team members in areas other than their own specialty.* Training team members in roles outside of their own job position is known as cross-training. The three different forms of cross-training are (a) Lecture/Presentation, which involves a team member communicating or presenting to others aspects of their functional roles and responsibilities; (b) Job Shadowing, which involves team members, particularly novice members shadowing a more experienced team member; and (c) Position Rotation, which involves individuals temporarily assuming the roles of other team members.

Trust in Teams and Incident Response Multiteam Systems. The CSIRT community has placed a significant emphasis on trust as an import factor for collaboration in incident response, one that was confirmed by our project findings. CSIRTs with high levels of trust facilitate faster threat mitigation with better, more novel solutions due to the conditions created by team leaders. For CSIRTs, trust can exist at multiple levels, including (a) Trust between CSIRT members, (b) Trust between CSIRT leaders and subordinates; (c) Trust between teams in an CSIRT MTS; and (d) Trust between organizations. Our findings have concluded that a series of exercises can be used by CSIRT managers to build trust in their teams, MTSs, and between organizations.

- *Provide structured opportunities for CSIRT members to learn about the expertise, experiences, and functional backgrounds of other members.* When CSIRTs are newly formed, or when members have not previously worked together, building perceptions of shared competence is an important first step in developing team trust. Disclosing unique skills and experiences related to these roles demonstrates that all team members are competent in their roles and can be counted on to perform tasks. Managers should encourage team members to engage in frequent interaction and information conservations where they exchange information about the following: backgrounds, work experiences, and (some) personal information that emphasizes shared goals and interest in establishing a good relationship.
- *Establish clear individual and team goals, roles, and performance standards.* Developing perceptions of shared competence requires managers to set clear team goals and ensure that members have a clear sense of team goals, their roles in meeting these goals, and the performance standards that indicate goal accomplishment. This will foster increased dependability and reliability within the team. In addition to considering the use of a chartering strategy and pre-briefing, managers should also clearly define team goals for a specific period of time (e.g., monthly) and ask each member to provide a list of goals. Based on team goals, each team member should specify their individual goals and demonstrate alignment with the team's mission. Managers should meet with the team on a regular basis to remind the team of goals, evaluate progress and provide feedback.
- *Establish norms for communication transparency in teams.* The first two strategies in this section help establish swift trust and establish the basis for further trust development. Deeper levels of trust begin when managers create and enforce a climate for communication transparency. Team members look to the leader for expectations of how they should behave. If CSIRT managers model openness and honesty in their communications with others, then their subordinates will be more likely to do the same. Managers should also enforce a norm for communication transparency by reacting swiftly to violations of this norm. If team members display a reluctance to be open in their interactions with their colleagues, managers should have a "clearing the air" meeting with those particular individuals, with team leads, or, if necessary, with the

CSIRT as a whole. The tone of such meetings should be constructive and supportive, with the purpose of addressing issues that are fostering careful disclosure rather than transparency in communications within the team.

- *Utilize managerial actions that create a psychologically safe climate in the team.* When CSIRT managers create a psychologically safe climate, team members are more likely to generate novel ideas, explore new perspectives, and learn from mistakes. To create a psychologically safe climate, CSIRT managers should ensure that team members feel valued. They should encourage them to generate the novel ideas that are often necessary to resolve unusual incidents. Creating this atmosphere requires CSIRT managers to take time during meetings to invite all team members to offer opinions, as some might be hesitant to go against the majority. It is important for all team members to be present when discussing important information, to demonstrate inclusivity. Managers should also actively try to take on other team members' perspectives and weight all ideas equally to consider each opinion before coming to a decision. During this process, it is important to encourage team members to bring up difficult topics and reward them (e.g., with praise) for offering new solutions or ideas. Above all, a CSIRT manager must display non-defensive responses to questions and challenges.
- *Create opportunities for building strong social connections among CSIRT members to support conflict management.* Both swift trust and deep trust emerge from positive social relationships among CSIRT members. Conflict will always occur in CSIRTs. Yet, a manager can minimize the damage to trust that conflict can cause by helping the team develop stronger interpersonal ties early in the team's formation. This can be as simple as providing "ice-breaking" social activities early in the team's formation or as new members join. Managers should have regular team social activities (e.g., team lunches, sports activities), especially if the team is not new. Engaging the team (or multiple teams in an MTS) in training activities that improve conflict resolution will prime the CSIRT to handle conflict constructively when it arises.
- *Increase external connections and social networking to facilitate inter-team and interorganizational trust*. Inter-organizational trust can be built through consistent networking across organizational boundaries, which is key to enhancing CSIRT maturity. This level of networking can be done at annual professional meetings or regularly scheduled meetings among individuals from different organizations who need to work with one another.

Sustained Attention and Focus over Time. CSIRTs benefit when watch teams are vigilant and able to sustain attention throughout their shift, reducing the occurrence of missed critical events. Our interviews of cybersecurity professionals indicated that employees sometimes look for critical events over extended periods of time (e.g., "eyes on glass"). This runs into the cost-benefit question of sustaining attention versus the quality of work. Frequently, the longer one focuses on a single task the better the achievement of the goal, provided that sustained focus does not compromise cognitive endurance (e.g., fatigue). To improve sustained attention and focus over time, managers should implement as many of our recommended strategies as possible. However, some strategies might not be applicable to specific CSIRTs or might be too costly to implement. For instance, if shift lengths, rotations, and length of breaks cannot be changed, managers could nonetheless provide suggestions for employees regarding the best use of rest breaks (incorporating socialization, for example). Additionally, managers could select employees based upon their ability to sustain attention; however, managers first must validate employee selection tools to ensure that working memory and brief sustained attention (i.e., vigilance) tasks predict sustained attention in CSIRT employees. Managers need to determine the primary factor influencing employees' performance, such as whether employees come to work tired or lose steam throughout work shifts. Shift-length and shift-rotation decisions are useful strategies to

address employee fatigue whereas rest-break strategies address decreases in attention over the length of a work shift. All of these factors impact effective cybersecurity incident response, particularly during critical times that require sufficient attention and cognitive endurance.

- *Hire job applicants who display a capacity for sustained attention.* One way to maximize employee attentiveness is to hire individuals who are better able to sustain attention and focus throughout their shifts. Selecting employees with higher levels of attention could be particularly beneficial for those teams whose tasks predominantly include surveillance tasks, such as monitoring and watch teams. It is difficult to predict individual differences in sustained attention using measures of personality or intelligence. We suggest managers use an employee selection test. Two measures, in particular, could prove useful in predicting an employee's sustained attention throughout the work shift. The first is a "working memory task," which measures the portion of memory that allows temporary storage of verbal or visual information. The second measure involves "brief sustained attention tasks." Performance on these tasks can predict employees' performance on longer sustained attention tasks, such as the monitoring task involved in incident response.
- *Encourage employees to incorporate rest breaks into their shifts.* Our interactions with CSIRT members pointed to the importance of periodic rest breaks during the workday. This strategy is practiced among cybersecurity professional in Europe where a periodic break is endorsed, most often a coffee break. We propose that organizations and managers should provide suggestions to employees about how to incorporate rest breaks into their schedules and encourage employees to take more consistent and regular rest breaks. CSIRT managers should encourage employees to take approximately one 15-minute break every two hours. Managers should also allow employees some latitude regarding when to take breaks, rather than forcing adherence to a rigid break schedule. A rigid break schedule can result in increased emotional strain for employees, possibly resulting from employees being interrupted in the middle of complex tasks. To provide a truly restorative setting during breaks, natural settings have been found to contribute to the replenishment of attention. Researchers found that reaction time became faster and attention increased when participants were exposed to a picture of nature compared to pictures of urban scenes. Additionally, socialization can be important to rest breaks. Informal interactions between employees can be a source of stimulation and variety in the work environment.
- *Shift design – create a shift plan that reduces sleep disturbances and maximizes attentiveness.* Our interviews with cybersecurity professionals demonstrated that shift lengths (e.g., 8-hour versus 12-hour shifts) and shift rotations (e.g., morning > afternoon > night > morning versus morning > night > afternoon > morning) differ across CSIRTs. Shifts should be implemented in a way that minimizes sleep disturbances and fatigue among employees. To improve sustained attention, managers should try to schedule employees for 8-hour work shifts as opposed to 12-hour shifts. Managers should seek to implement "rapid shift rotations," where possible. Shift rotation implies that shifts change based on a set schedule, and shift rotation speed refers to the number of consecutive work shifts until an employee's shift changes (e.g., the start and end time of the shift changes). Managers should use rapid shift rotations to increase employee alertness and reduce fatigue. This requires changing shifts every week or couple of days rather than after several weeks. A final critical consideration in shift design involves "shift rotation direction." Shifts typically rotate in a forward or backward direction. When possible, managers should use forward shift rotation (i.e., morning > afternoon > night > morning) rather than backward shift rotations (i.e., Morning > night > afternoon

> morning). Research indicates that people acclimate more easily to time zone changes that move clockwise or westward.

Continuous Learning in Incident Response. A continuous, positive learning environment is essential in cybersecurity incident response. CSIRTs are fast-moving. Analysts face rapidly changing threats and respond to increasingly novel situations. To keep pace, CSIRT analysts must utilize their individual inventiveness, and managers need to create systems and institutions that harness this ingenuity. This dynamic demands that cybersecurity analysts and teams constantly learn new skills. Such learning must occur across all levels: individual, team, and MTS.

Learning is not limited to individual skill development. CSIRTs need to place a high value on stored knowledge and must reach collective understanding of constantly evolving conditions. Individual team members and component teams often must adapt by changing their behaviors or worldviews. Managers can foster this process by establishing a trusting environment where individual team members feel confident to share their ideas. Our research has found four key strategies to create a positive learning environment within CSIRTs:

- *Selection of individuals who are creative and curious.* Curiosity results in information seeking and leads to learning, while creativity leads to explorations of novel directions, modifying and extending known solutions. Hiring people who are creative and curious is one approach for improving these attributes in a CSIRT. The selection of job applicants could be based on previous experience, structured interview questions, or responses to a psychological test.
- *Leader behaviors to encourage learning.* Leaders have the ability to encourage creativity and curiosity behaviors. One of the managers we interviewed indicated that he deliberately assigned analysts to work on special development projects, allowing them to show their creativity. Managers can also encourage CSIRT professionals to self-assess their own skills and knowledge. Based on self-assessment, they can plan their own learning activities, which can lead to increased confidence and better performance. Managers who encourage employees to establish goals and development opportunities create a feedback-seeking environment. This creates the opportunity to reward employees for learning new skills. Selfassessment and goal creation is also useful for teams. Managers should encourage teams to reflect on events and identify where changes are needed by holding debriefings, also referred to as after-action reviews.
- *Design work to enhance learning and development.* Work design refers to the organization of an employee's total role within a team. It can include the job tasks they perform, other activities they may engage in, relationships with others relevant to getting their jobs done, and the responsibilities in accomplishing their overall role. Work design has been demonstrated to affect workers' motivation as well as their learning and development. Research has shown that allowing CSIRT analysts autonomy over their working methods and pace of work can improve performance. Managers should design cybersecurity work roles around tasks that use a variety of skills, which has been shown to increase job performance. One of the most important factors in promoting learning is to put in place mentoring programs, which can help CSIRT professionals identify networking and learning opportunities.
- *Development of professional networking skills.* CSIRT managers should help their employees develop networking skills, which aid developmental growth. There are three factors to be considered in establishing a professional network for developmental purposes: (a) Assessment, where members in the network can provide relevant information and feedback on their developmental progress; (2) Challenge, where members of the network can get individuals to move beyond their comfort zones; and

(3) Support, where members of the network can provide support, helping individuals manage the challenges faced in increasing their knowledge, skills, and abilities. Managers can also facilitate guided discovery learning. Instead of traditional learning approaches (e.g., lectures, videos, or manuals), in discovery learning workers construct their own understandings through experimentation and exploration. Managers can facilitate discover learning using the examples in the chapter titled Continuous Learning in Incident Response in the Handbook located at http://calctraining2015.weebly.com/the-handbook.html. Lastly, error management training can be a useful mechanism for CSIRT managers to increase team members' comfort with admitting to and learning from mistakes.

5.0 Conclusions

Assessment Exercises & Improvement Strategies

The research team prepared Assessment Exercises and Improvement Strategies to assist CSIRT managers in evaluating and improving their teams. They are organized by chapter in the Handbook. Developed in response to this study's key findings, these assessmentquestions should serve as prompts for managers to gain insights into their team's functionality and effectiveness. The Improvement Strategies reflect our recommendations for improving team performance. Our research found common themes, gaps, opportunity costs, and areas for improvement across CSIRTs.

Content and Structure of the Handbook

The unique quality of this Handbook lies in the fact that we bring scientifically grounded approaches from organizational science to understanding CSIRT collaboration processes and offer empirically-determined strategies to improve these processes. We interviewed cybersecurity professionals across a variety of domains, responsibilities, and countries to identify key factors related to effective collaboration and connected them with proven strategies in the organizational sciences that influence team success. The result is a Handbook that is practical in use, but heavily grounded in science. The strategies provided vary in their relevance and application due to differences among CSIRTs. Where possible, we provide cost and benefit insights about our recommendations to help managers decide which strategies might be most effective for their teams (based on available resources). This Handbook includes eleven chapters that address various themes identified from our research program. The introductory chapter highlights the importance of social dynamics for incident response and summarizes these themes. This chapter also describes the methods used in our research. Topics related to the collaborative nature of incident response work and the environment in which such work occurs are covered in several chapters. "The Social Maturity of CSIRTs and Multiteam Systems" chapter provides an overview of the collective nature of cybersecurity work with a focus on CSIRTs as MTSs. Managers can then map out their own CSIRT as an MTS to focus on teams that work closely together. The chapter titled "Measuring and Evaluating CSIRT Performance" addresses how cybersecurity performance is measured and evaluated, issues with current approaches to performance measurement, and strategies for designing a comprehensive performance measurement program for the entire CSIRT. In the chapter titled "Decision-making in CSIRTs," we address how cybersecurity professionals make critical decisions, challenges faced when making critical decisions, and strategies to improve decision-making.

In the following chapters, we elaborate on individual and social drivers of effective incident response. We begin with a chapter titled "Communication Effectiveness in Incident Response," which describes how to develop communication skills among team members and enhance team and MTS communication. We provide insights into how communication strategies enhance information sharing within and between teams of cybersecurity professions in the next chapter titled "Information Sharing in

Incident Response." Enhancing collaborating problem solving among individuals and teams in incident response is addressed in the next chapter titled "Collaborative Problem Solving in Incident Response." Subsequent chapters cover topics related to persistent excellence during incident response. "Shared Knowledge of Unique Expertise" describes how individuals and teams can build shared knowledge of unique expertise, which helps CSIRT members identify which persons to call on for particular advice on how to address different kinds of incidents. Trust and psychological safety serve as the primary foundation upon which many individual, team, and MTS interactions occur. Methods for building trust among CSIRTs and MTS members (including those from other CSIRTs and agencies), as well as developing an environment of psychological safety are reviewed in the chapter titled "Trust in Teams and Incident Response Multiteam Systems." How individuals and teams can sustain attention and focus throughout lengthy periods of incident management is covered in "Sustained Attention and Focus over Time during Incident Response." The Handbook concludes with the chapter titled "Continuous Learning in Incident Response," which contains information on how to establish and support a learning climate that encourages CSIRTs and their members to continually adapt to changing conditions.

In the Handbook chapters, we include information on individual knowledge, skills, abilities, and other characteristics (KSAOs) necessary for effective cybersecurity incident response. These KSAOs include technical skills, cognitive abilities, social skills and other personal attributes necessary to engage individuals in effective and collaborative incident response. Managers can use these KSAOs to help determine the areas in which their CSIRT is strong or lacking, which can aid hiring decisions.

For each chapter, we provide "key themes" to highlight the main points. We begin each chapter with a brief introduction to the topic, followed by Assessment Exercises that can help readers decide if the topic may be an area for improvement in their respective CSIRTs. Prior to describing several recommendations for each topic, we provide background knowledge (e.g., definitions) and information from both the cybersecurity and organizational psychology domains (e.g., research findings, references) for those readers who are more interested in the data and results from our research. Evidence-based strategies are then provided to guide CSIRT managers on the use of various tools and training to develop and improve the social interactions of their team members. On occasions where our recommendations have yet to be rigorously tested, we provide guidelines for how to determine their effectiveness and relevance (for example, Appendix C: "Hiring and Training CSIRT Employees: Validation Considerations"). We do not recommend implementing such strategies until their effectiveness is determined. This Handbook includes several appendices that support information addressed throughout the chapters (e.g., how to validate selection tools, topical white papers, and a CSIRT performance taxonomy). The full Handbook with appendices can be downloaded at http://calctraining2015.weebly.com/thehandbook.html .

6.0 Selected References

9/11 Commission staff statement No.17. (2001). Improvising a homeland defense. Retrieved from: http://govinfo.library.unt.edu/911/staff_statements/staff_statement_17.pdf

Abrams, M., & Weiss, J. (2008). Malicious control system cyber security attack case study–Maroochy Water Services, Australia. *McLean, VA: The MITRE Corporation*.

Barrett, D., & Yadron, D. (2015, February 22). Sony, U.S. agencies fumbled after cyberattack. Retrieved from http://www.wsj.com/articles/sony-u-s-agencies-fumbled-after-cyberattack-1424641424

Bowen, P., Hash, J., and Wilson, M. (2006). *Information security handbook: A guide for managers* (NIST Special Publication 800-100). National Institute of Standards and Technology: Gaithersburg, MD.

Brooks, J. M., Bodeau, D., & Fedorowicz, J. (2013). Network management in emergency response articulation practices of State-level managers—Interweaving up, down, and sideways. *Administration & Society, 45*(8), 911-948.

Cascio, W. F. and Aguinis, H. (2010). Applied psychology in human resource management (7th Ed). New York: Prentice Hall.

Chen, T. R., Shore, D. B., Zaccaro, S. J., Dalal, R. S., Tetrick, L. E., & Gorab, A. K. (2014). An organizational psychology perspective to examining computer security incident response teams. *IEEE Security & Privacy*, (5), 61-67.

De Wolf, D., & Mejri, M. (2013). Crisis communication failures: The BP case study. *International Journal of Advances in Management and Economics, 2*(2), 48-56.

DeChurch, L. A., & Marks, M. A. (2006). Leadership in multiteam systems. *Journal of Applied Psychology*, *91*(2), 311-329.

DeChurch, L. A., Burke, C. S., Shuffler, M. L., Lyons, R., Doty, D., & Salas, E. (2011). A historiometric analysis of leadership in mission critical multiteam environments. *The Leadership Quarterly, 22*(1), 152-169.

Duncker, K., & Lees, L. S. (1945). On problem-solving. *Psychological monographs*, *58*, i-113.

Dwyer, J., Flynn, K., & Fessenden, F. (2002, July 6). Fatal confusion: A troubled emergency response; 9/11 exposed deadly flaws in rescue plan. Retrieved from http://www.nytimes.com/2002/07/07/nyregion/fatal-confusion-troubled-emergency-response9-11-exposed-deadly-flaws-rescue.html

Festinger, L. (1950). Informal social communication. Psychological Review, 57, 271-282.

Fleishman, E. A., & Quaintance, M. K. (1984). *Taxonomies of human performance: The description of human tasks*. Orlando, FL: Academic Press.

Goldernberg, S. (2010, December 2). BP oil spill blamed on management and communication failures. Retrieved from http://www.theguardian.com/business/2010/dec/02/bp-oil-spill-failures Goodwin, G. F., Essens, P. J. M. D., & Smith, D. (2012). *Multiteam systems in the public sector* (pp. 5380). Taylor & Francis.

Grimaila, M. R., Schechtman, G., Mills, R. F., & Fortson, L. W. (2009, January). Improving cyber incident notification in military operations. In *IIE Annual Conference. Proceedings* (p. 2357). Institute of Industrial Engineers-Publisher.

Harvey JR. J. C. (2012). *Cyber forces: Commander's cyber security and information assurance handbook*. Norfolk, VA.: Department of the Navy:

Illman, P., & Gailey, G. (2012). *Pilot's radio communications handbook sixth edition*. New York: McGraw Hill Professional.

Janis, I. (1972). Victims of groupthink. Boston: Houghton Mifflin.

Killcrece, G., & Ruefle, R. (2008). Creating and managing computer security incident handling teams (CSIRTs). Software Engineering Institute, Carnegie Mellon University: Pittsburgh, PA.

Kohn, L. T., Corrigan, J. M., & Donaldson, M. S. (1999). *To err is human. Building a safer health system*. Committee on Quality of Health Care in America. Washington, DC: Institute of Medicine.

Kozlowski, S. W., & Ilgen, D. R. (2006). Enhancing the effectiveness of work groups and teams. *Psychological Science in the Public Interest*, *7*(3), 77-124.

Ministry of Security and Justice, the Netherlands; Federal Office for Information Security, Germany; Swedish Civil Contingencies Agency, Sweden. (2014). *International case report on cyber security incidents: Reflections on three cyber incidents in the Netherlands, Germany and Sweden*.

Mitropoulos, S., Patsos, D., & Douligeris, C. (2006). On incident handling and response: A state-of-the-art approach. *Computers & Security*, *25*, 351-370.

NICE. (2013).The national cyber security workforce framework 1.0. Retrieved from http://csrc.nist.gov/nice/framework/national_cyber security_workforce_framework_03_2013_version1_0_for_printing.pdf

Pfleeger, S. L., Fenton, N., and Page, S. (1994). Evaluating software engineering standards. *Computer, 27*(9), 71-79.

Reinhardt, W., Schmidt, B., Sloep, P., & Drachsler, H. (2011). Knowledge worker roles and actions—results of two empirical studies. *Knowledge and Process Management*, *18*(3), 150-174.

Sawalha, I. H. S. (2014). Collaboration in crisis and emergency management: Identifying the gaps in the case of storm 'Alexa'. *Journal of Business Continuity & Emergency planning*, *7*(4), 312-323.

Scott. B. C. (2012). Broadening army leaders for the volatile, uncertain, complex and ambiguous environment. Unpublished master's thesis, U.S. Army War College, Carlisle, PA.

Steiner, I. D. (1972). *Group processes and productivity*. New York: Academic Press.

Steinke, J., Bolunmez, B., Fletcher, L., Wang, V., Tomassetti, A. J., Repchick, K. M., ..., & Tetrick, L. E. (2015). Improving cyber security incident response team effectiveness using teams-based research. *Security & Privacy, IEEE*, *13*(4), 20-29.

Studdert, D. M., Brennan, T. A., & Thomas, E. J. (2002). What have we learned from the Harvard Medical Practice Study? In M. M. Rosenthal &K.M. Sutcliffe (Eds.), Medical error: What do we know? What do we do? (pp. 3−33). San Francisco: Jossey-Bass.

The Swedish Civil Contingencies Agency. (2012). Reflections on civil protection and emergency preparedness during major IT incidents: A study of societal impact following the disruption at Tieto in November 2011 (Publication No. MSB 435-12). Retrieved from: https://www.msb.se/RibData/Filer/pdf/26243.pdf

U.S. Department of Defense, National Guard. (2005). After-action review: Hurricane response. September 2005 (NGB J7).

U.S. Department of Homeland Security, Federal Emergency Management Agency. (2005, September 30). Urban search and rescue operations completed: Hurricane Katrina urban search and rescue teams are due to return home. Retrieved from https://www.fema.gov/newsrelease/2005/09/30/urban-search-and-rescue-operations-completed.

U.S. Executive Office of the President, U.S. Assistant to the President for Homeland Security and Counterterrorism. (2006).*The Federal response to Hurricane Katrina: Lessons learned.* (PREX 1.2:K 15) Washington, D.C.: White House.

Walker, G. H., Gibson, H., Stanton, N. A., Baber, C., Salmon, P., & Green, D. (2006). Event analysis of systemic teamwork (EAST): A novel integration of ergonomics methods to analyze C4i activity. *Ergonomics*, *49*(12-13), 1345-1369.

Wertheimer, M. (1954). *Productive thinking*. New York: Harper & Row.

West-Brown, M. J., Stikvoort, D., Kossakowski, K. P., Killcrece, G., Ruefle, R., & Zajicek, M. (2003). *Handbook for computer security incident response teams (CSIRTs) (2nd Ed.).* Pittsburgh, PA: Carnegie Mellon Software Engineering Institute.

Wolf, L. J. (2004). Can you handle the headaches? Analyzing and optimizing the effectiveness of the incident management process. *Information Systems Security*, *13*(5), 9-20.

Zaccaro, S. J., Marks, M. A., & DeChurch, L. (Eds.). (2012). *Multiteam systems: An organization form for dynamic and complex environments*. New York: Routledge.

Zaccaro, S. J., Dalal, R. S., Tetrick, L. E., & Steinke, J. A. (Eds.). (2016) *Psychosocial Dynamics of Cyber Security.* New York: Routledge.